УДК 342.9
DOI https://doi.org/10.32782/2523-4269-2022-81-4-1-119-122

Онопрієнко Станіслав Григорович,
кандидат юридичних наук
(Військовий інститут Київського національного університету імені Тараса Шевченка, м. Київ)
ORCID: https://orcid.org/0000-0002-5524-1798

ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У СТРАТЕГІЇ НАЦІОНАЛЬНОЇ БЕЗПЕКИ РЕСПУБЛІКИ ПОЛЬЩА

Статтю присвячено визначенню сутності та напрямів інформаційної безпеки у Стратегії національної безпеки Республіки Польща 2020 року.
З'ясовано, що інформаційна безпека виступає важливим елементом національної безпеки сучасної держави, що обумовлено як постійним розвитком інформаційних технологій, так і постійним ускладненням та вдосконаленням гібридних загроз та інформаційно-психологічних операцій. Встановлено, що у Республіці Польща проблемам забезпечення інформаційної безпеки як складової частини національної приділяється достатня увага, про що свідчить зміст Стратегії національної безпеки Республіки Польща 2020 року. До особливостей відображення проблем інформаційної безпеки у вказаному правовому документі віднесено такі: людиноцентричність, що знаходить свій прояв як у напрямах діяльності з кібербезпеки, так і у заходах із захисту інформаційного простору; комплексне розуміння інформаційного простору як поєднання віртуальної, фізичної та когнітивної складової частин; підкреслювання важливості створення єдиної системи стратегічних комунікацій держави, яка мала б риси єдності та послідовності, а також попереджувальний характер впливів; значущість педагогічного фактору протидії агресивним інформаційним впливам (для представників як державного, так і недержавного сектору).
Ключові слова: *інформаційна безпека, національна безпека, Стратегія національної безпеки, Республіка Польща, інформаційні правовідносини, стратегічні комунікації, інформаційний простір, інформаційне законодавство.*

Постановка проблеми в загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. Повномасштабна збройна агресія Російської Федерації проти України сприяла консолідації зусиль нашої держави з країнами Європейського Союзу, особливе місце серед яких займає Республіка Польща. Польські органи влади та громадянське суспільство багато років демонструють послідовну політику адвокації України в структурах Європейського Союзу та Північноатлантичного Альянсу, підтримку нашої держави як у сфері воєнної, так і гуманітарної політики. У затвердженій у 2020 році Стратегії національної безпеки Республіки Польща визначено особливості дій цієї держави у середовищі безпеки, яке характеризується невизначеністю та непередбачуваністю, оскільки зростає кількість загроз та викликів безпеці різного характеру, найсерйознішою загрозою є неоімперська політика влади Російської Федерації, яка також реалізується із застосуванням військової сили [1]. Враховуючи значущість узгодження політик Республіки Польща та України у сфері забезпечення інформаційної безпеки, дослідження польського досвіду, відображеного у Стратегії національної безпеки Республіки Польща 2020 року, уявляється нам вельми важливим. Водночас в українських правових дослідженнях ця проблематика ще не набула широкого висвітлення.

Аналіз останніх досліджень і публікацій, у яких започатковано розв'язання визначеної проблеми. Стратегічні засади забезпечення інформаційної безпеки в сучасних умовах розглядав у своїх роботах В. Новицький, який на підставі дослідження гібридних інформаційних загроз та викликів, які поширює Російська Федерація, та концептуальних засад державної інформаційної політики в умовах сучасності робить висновок, що саме стратегічне планування у сфері забезпечення інформаційної безпеки дає змогу значно підвищити ефективність та якість державного управління у цій сфері. Стратегічне планування, на думку вченого, повинно розглядатися усіма органами державної влади та управління як універсальний інструмент, завдяки якому можливо забезпечити реалізацію актуальних державних завдань у сфері забезпечення інформаційної безпеки, у тому числі й з використанням механізму державно-приватного партнерства [2]. Досвід правового забезпечення інформаційної безпеки в країнах східного партнерства Європейського Союзу, зокрема у Молдові та Грузії, дослідила у своїх працях О. Золотар, яка обґрунтувала доцільність вивчення та використання їхнього досвіду у сфері інформаційної безпеки з перспективи вдосконалення правового забезпечення відповідних відносин в Україні, а також звернула увагу на інформаційний супровід впровадження нових технологій в процеси демократизації, оскільки самі по собі інструменти не творять ані державу, ані суспільство, а їх сприйняття та ефективне використання громадянами має значний потенціал і для держави, і для кожного члена суспільства зокрема [3].

О. Довгань і Т. Ткачук дослідили концептуальні засади законодавчого забезпечення інформаційної безпеки України в контексті принципу, відповідно до якого

основною метою забезпечення інформаційної безпеки є створення безпечного інформаційного середовища. А для цього захищати національні інтереси й цінності, виходячи з виявлення загроз і намірів противника, замало. Даний підхід передбачає також протидію та активні контрзаходи у процесі забезпечення інформаційної безпеки держави. Науковці запропонували власну модель законодавчого забезпечення інформаційної безпеки та окреслили її структурні особливості [4]. Однак слід сказати, що проблематика інформаційної безпеки як складової системи системи національної безпеки Республіки Польща ще недостатньо досліджена в українській правовій науці.

Мета статті – визначення особливостей закріплення сутності та напрямів реалізації інформаційної безпеки у Стратегії національної безпеки Республіки Польща.

Виклад основного матеріалу. Республіка Польща приділяє багато уваги проблемам забезпечення інформаційної безпеки в різних сферах суспільних відносин. Як і в інших країнах, вказана проблематика спочатку активно досліджувалася як одна зі частин складових безпеки підприємницької діяльності. Так, польський вчений Л. Кільтика, вивчаючи питання управління безпекою інформації, ще у 2003 році запропонував своє бачення вдосконалення управління інформаційною безпекою в організаціях, приділивши при цьому увагу існуючим формам безпеки передачі інформації, нормативно-правовим актам, що регулюють захист інформації, дослідивши багатосторонню безпеку та політику інформаційної безпеки [5].

Значний імпульс дослідження особливостей інформаційної безпеки спостерігався в контексті запровадження в Республіці Польща стандарту якості ISO/IEC 27001:20051, який визначає управління системами інформаційної безпеки, засноване на процесі оцінки ризиків. Як зазначають польські дослідники Я. Лучак і М. Тибурський, бурхливий і дуже динамічний розвиток інформаційних технологій, а також стрімко зростаюча кількість оброблених даних змусили шукати рішення, що дозволяють ефективно керувати інформацією, враховуючи пов'язані з нею ризики [6]. Спираючись на положення Конституції Республіки Польща 1997 року, зокрема, її ст. 47, яка визначає, що кожен має право захищати своє особисте і сімейне життя, честь і добре ім'я, вирішувати питання про своє особисте життя, ч. 1 ст. 51, відповідно до якої ніхто не може бути зобов'язаний розкривати інформацію, що стосується нього, інакше відповідно до закону, законодавства про захист персональних даних та інших правових актів вчені описали правову систему забезпечення інформаційної безпеки на рівні організації, модель якої могла бути використана різними підприємствами залежно від галузевої специфіки [1].

Однак проблеми забезпечення інформаційної безпеки держави, безумовно, є більш складними та багатогранними, ніж забезпечення інформаційної безпеки організації. У Республіці Польща це усвідомлювалося на державному рівні і знаходило своє відображення у низці правових документів у галузі національної безпеки. У затвердженій 20 травня 2020 року Стратегії національної безпеки Республіки Польща вказано, що держава створює умови для реалізації національних інтересів і досягнення цілей у сфері національної безпеки відповідно до цінностей, які включають: незалежність і суверенітет держави, безпеку громадян, свободи і права людини і громадянин, людську гідність, справедливість, національну та демократичну ідентичність і спадщину, верховенство права, солідарність, міжнародний порядок, заснований на принципах міжнародного права та охорону навколишнього середовища. Вищезазначені національні інтереси є основою національної безпеки Республіки Польща. Їх реалізація здійснюється шляхом досягнення результуючих стратегічних цілей, які передбачають планування та виконання конкретних завдань та володіння та використання відповідних сильних сторін, ресурсів та можливостей [1].

Важливість інформаційної безпеки як складової частини національної безпеки Республіки Польща підтверджується тим фактом, що їй присвячено 2 із 5 підрозділів розділу 1 Стратегії національної безпеки (Збройним Силам Республіки Польща у вказаному розділі присвячено один підрозділ). Четвертий підрозділ розділу 1 досліджуваної Стратегії має назву «Кібербезпека» і визначає мету діяльності у відповідній сфері як підвищення рівня стійкості до кіберзагроз та підвищення рівня захисту інформації в державному, військовому та приватному секторах і просування знань і позитивної практики, які дозволяють громадянам краще захищати свою інформацію [1]. На нашу думку, заслуговує на увагу концентрація уваги нормотворця на людському факторі у кібербезпеці. Не є секретом, що у багатьох дослідженнях, присвячених проблемам кібербезпеки, увага концентрується у першу чергу на діяльності, потребах та інтересах держави, а поведінка громадянина оцінюється як така, яка має відповідати певним, встановленим державою стандартам. Водночас зрозуміло, що жодна система кібербезпеки як складова частина інформаційної безпеки не буде надійною, якщо людина як користувач кіберсистем, відправник чи отримувач інформації, керівник або підлеглий, не усвідомить та не інтеріоризує основні правила роботи з інформаційними системами, відомостями та даними. Заслуговує на увагу, що розуміння сутності кібербезпеки у Стратегії національної безпеки Республіки Польща в цілому відповідає ролі людини як основоположного елементу системи кібербезпеки, що детермінує як міцність, так і вразливості систем захисту. Про це, зокрема, свідчить зміст шести основних напрямів реалізації завдань з кібербезпеки, якими є:

1) підвищення рівня стійкості інформаційних систем, що використовуються в публічній сфері, і приватних, а також військових і цивільних, і досягнення здатності ефективного запобігання і боротьби з кіберзагрозами та реагування на них;

2) зміцнення обороноздатності держави шляхом забезпечення постійного національного розвитку системи кібербезпеки;

3) розвиток вмінь ведення повного спектру військових дій у кіберпросторі;

4) розвиток національних можливостей у сфері тестування, дослідження, оцінки та сертифікації рішень та послуг у сфері кібербезпеки;

5) розвиток компетентності, знань та усвідомлень загроз і викликів серед адміністративного персоналу, громадськості та в суспільстві у сфері кібербезпеки;

6) зміцнення та розширення потенціалу держави, наприклад, через розробку місцевих рішень у сфері кібербезпеки та проведення робіт за державного фінансування, дослідження та розробки в області сучасних технологій, наприклад, автоматизоване навчання, Інтернет речей, широкосмугові мережі фіксованого та мобільного зв'язку (5G) і наступних поколінь), включаючи співпрацю з університетами та науковими установами та компаніями як державного, так і приватного секторів [1].

Аналіз змісту наведених напрямів свідчить також про усвідомлення важливості навчання у галузі кібербезпеки не лише державних службовців та військовослужбовців, а широких верств населення, всього громадянського суспільства. Такий системний підхід, на який вже звертали увагу дослідники [7], на нашу думку, може дозволити втілити положення Стратегії у реальність. І державні службовці, і військовослужбовці, і представники правоохоронних та розвідувальних органів є частиною суспільства, а їхні професійні знання, вміння та навички стають результатом багатолітнього навчання, розпочинаючи з дитячого віку. Неможливо на якомусь етапі отримати компетентних фахівців з кібербезпеки, якщо все суспільство має низький рівень інформаційної грамотності. І навпаки, підвищуючи рівень інформаційних знань, вмінь та навичок всього суспільства, можна вплинути на фаховий рівень професіоналів у сфері кібербезпеки.

П'ятий підрозділ розділу 1 Стратегії національної безпеки Республіки Польща має назву «Інформаційний простір» і містить мету «забезпечення безпечного функціонування держави та громадян в інформаційному просторі». Реалізація вказаної мети передбачається в таких напрямах:

1) на стратегічному рівні створити можливості для захисту інформаційного простору (в т.ч. для системної боротьби з дезінформацією), що розуміється як взаємопроникнення таких шарів простору: віртуального (системи, програмне забезпечення та прикладний рівень); фізичного (інфраструктура і обладнання) і когнітивного;

2) створення єдиної системи стратегічних комунікацій держави, завданням якої має бути прогнозування, планування та здійснення послідовної комунікаційної діяльності;

3) використання широкого спектру комунікаційних каналів і засобів масової інформації та інструментів розвідки та впливу на різні сфери національної безпеки;

4) проактивна протидія дезінформації шляхом нарощування потенціалу та процедур співпраці з інформаційними та соціальними медіа із залученням громадян та неурядових; організацій;

5) підвищення обізнаності громадськості про ризики маніпулювання інформацією через освіту в галузі інформаційної безпеки.

Серед наведених положень, на нашу думку, заслуговує на увагу розуміння інформаційного простору як поєднання віртуальної, фізичної та когнітивної складової. Таке визначення уявляється нам більш прагматичним, ніж певні розуміння означеної категорії в українській науці інформаційного права, де інформаційний простір вважається феноменом, що виник задовго до існування людини і призначений для задоволення потреб всіх живих істот [8, с. 166].

Важливим, на нашу думку, є визначення місця стратегічних комунікацій у системі забезпечення інформаційної безпеки. Ми підтримуємо думку, що досягнення високого рівня захищеності державного суверенітету, територіальної цілісності і демократичного конституційного ладу та інших життєво важливих національних інтересів від реальних і потенційних загроз в умовах експоненціального розвитку інформаційних технологій потребує переосмислення існуючих систем обміну інформацією, що зумовлює увагу до феномену стратегічних комунікацій [9, с. 158]. Значущим для будь-якої демократичної держави виступає також, як нам уявляється, підкреслювання ролі неурядових організацій у виконанні завдань із забезпечення інформаційної безпеки на національному рівні.

Висновки. Інформаційна безпека виступає важливим елементом національної безпеки сучасної держави, що зумовлено як постійним розвитком інформаційних технологій, так і постійним ускладненням та вдосконаленням гібридних загроз та інформаційно-психологічних операцій. У Республіці Польща проблемам забезпечення інформаційної безпеки як складової частини національної приділяється достатня увага, про що свідчить зміст Стратегії національної безпеки Республіки Польща 2020 року. До особливостей відображення проблем інформаційної безпеки у вказаному правовому документі слід віднести такі:

1) людиноцентричність, що знаходить свій прояв як у напрямах діяльності з кібербезпеки, так і в заходах із захисту інформаційного простору;

2) комплексне розуміння інформаційного простору як поєднання віртуальної, фізичної та когнітивної складових частин;

3) підкреслювання важливості створення єдиної системи стратегічних комунікацій держави, яка мала б риси єдності та послідовності, а також попереджувальний характер впливів;

4) значущість педагогічного фактору протидії агресивним інформаційним впливам (для представників як державного, так і недержавного сектору).

Подальші наукові дослідження мають передбачати вивчення ролі інформаційної безпеки в стратегіях національної безпеки держав Європейського Союзу та порівняння рівня реалізації визначених у них заходів.

Список використаних джерел

1. Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej: zatwierdzona w dniu 12 maja 2020 roku przez Prezydenta Rzeczypospolitej Polskiej, na wniosek Prezesa Rady Ministrów. URL: https://www.prezydent.pl/aktualnosci/wydarzenia/nowa-strategia-bezpieczenstwa-narodowego-rp-,1752 (дата звернення: 18.11.2022 р.).

2. Новицький В.Я. Стратегічні засади забезпечення інформаційної безпеки в сучасних умовах. *Інформація і право*. 2022. № 1(40). С. 111–118. DOI: https://doi.org/10.37750/2616-6798.2022.1(40).254349 (дата звернення: 18.11.2022 р.).

3. Золотар О.О. Досвід правового забезпечення інформаційної безпеки в країнах східного партнерства ЄС (Молдова, Грузія). *Lex portus*. 2017. № 3. С. 70–80.

4. Довгань О.Д., Ткачук Т.Ю. Концептуальні засади законодавчого забезпечення інформаційної безпеки України. *Інформація і право.* 2019. № 1.(28). С. 86–99.

5. Kiełtyka L. Zarządzanie bezpieczeństwem informacji. *Współczesne Zarządzanie*. 2003. № 3. С. 19–32.

6. Łuczak J., Tyburski M. Systemowe zarządzanie bezpieczeństwem informacji ISO/IEC 27001. Poznań: Wyd. Uniwersytetu Ekonomicznego w Poznaniu, 2009. 215 s. URL: https://jacekluczak.pl/images/download/Systemowe.pdf.

7. Khomiakov D., Khrystynchenko N., Shopina I., Zhukov S., Shpenov D. Cybersecurity: Legal and Organizational Support in Leading Countries, NATO and EU Standards**.** *Journal of Security & Sustainability Issues.* 2020/3/1. Volume 9, Issue 3. P. 977–992. URL: https://doi.org/10.9770/jssi.2020.9.3(22) (дата звернення: 18.11.2022 р.).

8. Фурашев В.М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності. *Інформація і право*. 2012. № 2. С. 162–169.

9. Шопіна І.М. Стратегічні комунікації як правова категорія: поняття та розвиток. *Наука і правоохорона*. 2020. № 2(48). С. 158–165.

References

1. Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej [National Security Strategy of the Republic of Poland:]: zatwierdzona w dniu 12 maja 2020 roku przez Prezydenta Rzeczypospolitej Polskiej, na wniosek Prezesa Rady Ministrów. URL: https://www.prezydent.pl/aktualnosci/wydarzenia/nowa-strategia-bezpieczenstwa-narodowego-rp-,1752 (data zvernennia 18.11.2022 r.).
2. Novytskyi, V. (2022). Stratehichni zasady zabezpechennia informatsiinoi bezpeky v suchasnykh umovakh [Strategic principles of ensuring information security in modern conditions]. *Informatsiia i pravo*, №1 (40): 111-118. DOI: https://doi.org/10.37750/2616-6798.2022.1(40).254349 (data zvernennia: 18.11.2022 r.).
3. Zolotar, O. (2017). Dosvid pravovoho zabezpechennia informatsiinoi bezpeky v krainakh skhidnoho partnerstva EU (Moldova, Hruziia) [Experience of legal provision of information security in the countries of the Eastern Partnership of the EU (Moldova, Georgia)]. *Lex portus,* № 3: 70-80.
4. Dovhan, O.; Tkachuk, T. (2019). Kontseptualni zasady zakonodavchoho zabezpechennia informatsiinoi bezpeky Ukrainy [Conceptual principles of legislative provision of information security of Ukraine]. *Informatsiia i pravo*, №1 (28): 86-99.
5. Kiełtyka, L. (2003). Zarządzanie bezpieczeństwem informacji [Information security management]. *Współczesne Zarządzanie*, № 3: 19-32.
6. Łuczak, J., Tyburski, M. (2009). Systemowe zarządzanie bezpieczeństwem informacji ISO/IEC 27001 [System information security management ISO/IEC 27001]. Poznań: Wyd. Uniwersytetu Ekonomicznego w Poznaniu,. 215 s. URL: https://jacekluczak.pl/images/download/Systemowe.pdf
7. Khomiakov, D., Khrystynchenko, N., Shopina, I., Zhukov, S., Shpenov, D. (2020). Cybersecurity: Legal and Organizational Support in Leading Countries, NATO and EU Standards. Journal of Security & Sustainability Issues, volume 9, issue 3: P.977-992. https://doi.org/10.9770/jssi.2020.9.3(22) (data zvernennia 18.11.2022 r.).
8. Furashev, V. (2012). Kiberprostir ta informatsiinyi prostir, kiberbezpeka ta informatsiina bezpeka: sutnist, vyznachennia, vidminnosti [Cyberspace and information space, cyber security and information security: essence, definition, differences]. *Informatsiia i pravo,* № 2: 162-169.
9. Shopina I. M. Stratehichni komunikatsii yak pravova katehoriia: poniattia ta rozvytok [Strategic communications as a legal category: concept and development]. *Nauka i pravookhorona*. 2020. № 2(48). S. 158-165.

Onopriienko Stanislav,
Candidate of Legal Sciences
(Military Institute of Taras Shevchenko
National University of Kyiv)
ORCID: https://orcid.org/0000-0002-5524-1798

PROBLEMS OF INFORMATION SECURITY IN THE NATIONAL SECURITY STRATEGY OF THE REPUBLIC OF POLAND

The article is devoted to defining the essence and directions of information security in the 2020 National Security Strategy of the Republic of Poland.

Arguments are given that information security is an important element of the national security of a modern state, which is due to both the constant development of information technologies and the constant complication and improvement of hybrid threats and information-psychological operations. This became especially important after the beginning of the full-scale aggression of the Russian Federation against Ukraine, which is accompanied by active propaganda and media threats from the enemy. Peculiarities of the development of the concept of information security have been investigated in studies devoted to ensuring the activities of business entities. Attention is focused on the greater complexity and branching of the information security of the state compared to the information security of the organization.

The article establishes that in the Republic of Poland, sufficient attention is paid to the problems of ensuring information security as a national component, as evidenced by the contents of the National Security Strategy of the Republic of Poland for 2020. The specifics of information security problems in the specified legal document include the following: people-centricity, which is manifested both in the areas of cyber security and in measures to protect the information space; comprehensive understanding of the information space as a combination of virtual, physical and cognitive components; emphasizing the importance of creating a single system of strategic communications of the state, which would have the features of unity and consistency, as well as the preventive nature of influences; the importance of the pedagogical factor of countering aggressive informational influences (for representatives of both the state and non-state sectors).

Key words: *information security, national security, National Security Strategy, Republic of Poland, information legal relations, strategic communications, information space, information legislation.*

Надіслано до редколегії 15.11.2022